

GNSS

LANpedusa

Vernuccio s346272, Vicari s349369, Vinesia s343189, Zanti s334098

1 INTRODUCTION

The main task of this laboratory exercise is to perform a comprehensive analysis of raw Global Navigation Satellite System (GNSS) measurements and Position, Velocity, and Time (PVT) solutions. This involves systematically collecting and evaluating GNSS data under a variety of environmental and signal conditions using the GNSS Logger application on an Android smartphone. The lab focuses on understanding how different factors—such as signal obstruction, urban environments, and simulated interference—affect the accuracy and reliability of PVT solutions.

2 METHODS

The collection of measurements was conducted in the inner courtyard of the Polytechnic, using the app "GNSS logger" with an Oppo Find X5, under different conditions: in an open-sky environment without and with battery mode, and inside a classroom. Then, modifying the file "ProcessGnssMeasScript.m", it was enabled the spoofing position and the spoofing delay. Finally, it was analyzed the case with an interference source, such as phone call. In order to examine our collection of data, are been reported plots like pseudoranges, carrier-to-noise density ratio, weighted least squares and bias clock offset.

3 RESULTS AND DISCUSSION

3.1 Task 3: open sky condition.

As part of our outdoor GNSS testing, we recorded and assessed positional data under open-sky conditions. The output, shown in Figure 1, highlights a noticeable level of positional spread, indicating limited precision. Upon further analysis, we observed key patterns that align with our expectations.

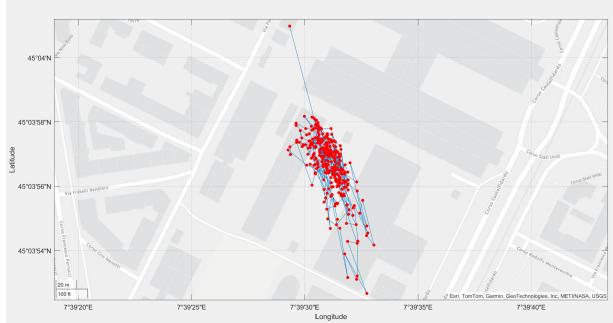


Figure 1.

Specifically, Figure 2 shows that approximately half of the recorded points lie within a 19.6-meter radius, which reflects a considerable positioning error. This level of deviation is likely the result of several contributing factors, such as standard limitations in GNSS receiver accuracy, signal reflections from nearby buildings (multipath), and environmental influences like atmospheric interference. This last aspect is caused by the fact that the measurement has been done in the classroom I's courtyard, which is located underground, then it's quite reasonable to have these types of inaccuracies. Frequent spikes in

horizontal speed—sometimes nearing 1 m/s—can be observed in the data, assessing that the smartphone is moving with different speed, but it's not and the last graph, which is related to HDOP, indicates that it's varying between 1 and and 2 with one peak up to 3. The presence of such fluctuations highlights how environmental factors can impact GNSS performance and reinforces the need to reduce multipath effects to achieve more accurate positioning data.

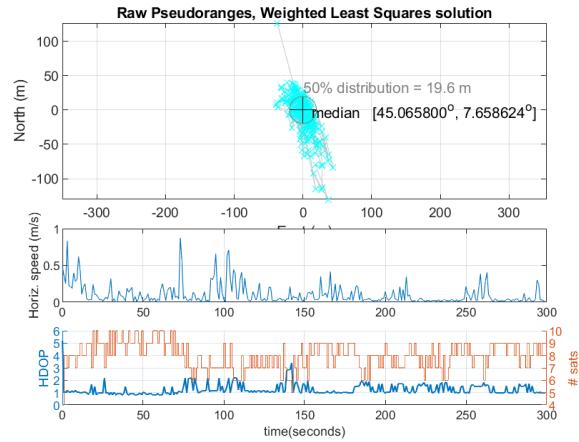


Figure 2.

As illustrated in Figure 3, several signals fall below the 30 dB.Hz mark, with satellite 17 consistently recording values under 25 dB.Hz. Such persistently weak signal strength can negatively affect the precision and stability of the resulting position estimates. The signal quality in GNSS is often assessed using the Carrier-to-Noise density ratio (C/No), which measures the strength of the carrier signal relative to the ambient noise level. This metric plays a key role in determining the reliability of satellite signal reception.

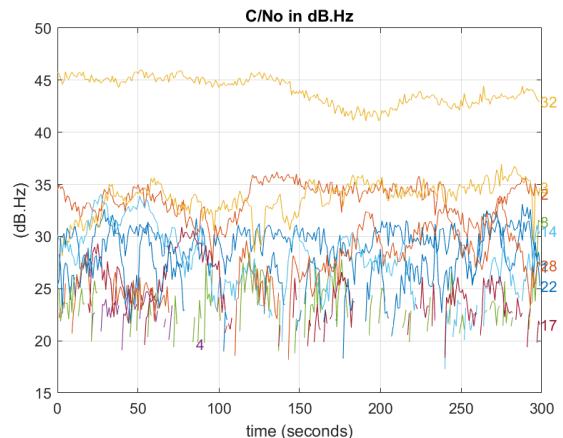


Figure 3.

3.2 Task 3: battery saving mode.

When the GNSS receiver is switched to power-saving mode, it is expected that both the update frequency and positional accuracy will be compromised in order to extend battery life. This is because the receiver reduces its sampling rate or even enters a sleep state, where the chip either shuts down or significantly lowers its activity, leading to clock discontinuities and, consequently, gaps in measurements.

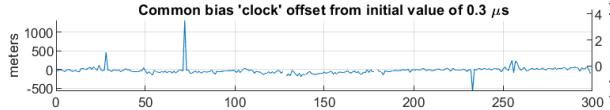


Figure 4.

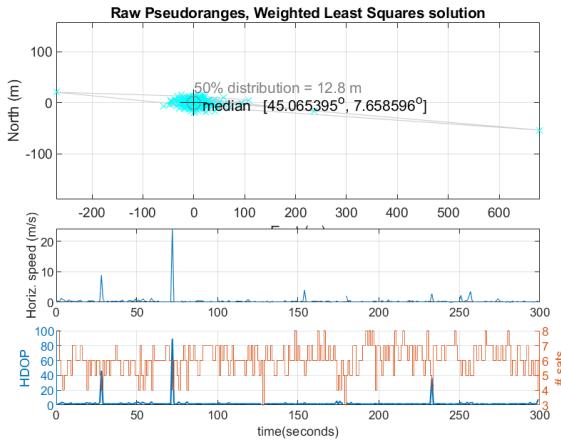


Figure 5.

Upon exiting the sleep mode, the receiver's Phase-Locked Loop (PLL) system begins to resample at a slower rate, which introduces a noticeable shift in the clock bias, as seen in Figure 4. Simultaneously, in HDOP graph occurs some spikes, as shown in Figure 5, due to the system's attempt to regain synchronization. This temporary loss of lock during the wake-up phase results in inaccuracies in both the time and position calculations.

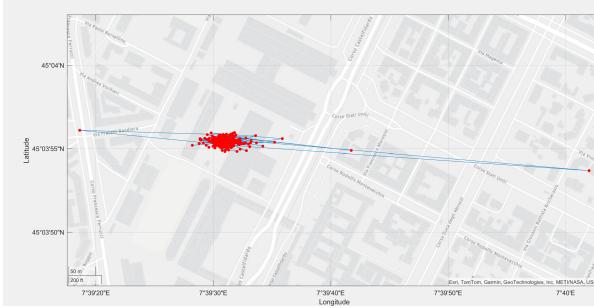


Figure 6.

As a result, the receiver is unable to provide precise positioning immediately after resuming normal operation. The uncertainty caused by this issue is clearly visible in Figure 6, where some measurements deviate significantly from the median, with some values reaching up to 700 meters away. Making a comparison between optimal condition and battery save mode, it can be seen from the Figures 7 and 8 that the values in the second case barely change, this is a consequence

of the principal characteristic of battery save mode. In fact, going deeper into the analysis, due to the discontinuous updates, all the data mostly remains to 0 with rare peaks when an update occurs.

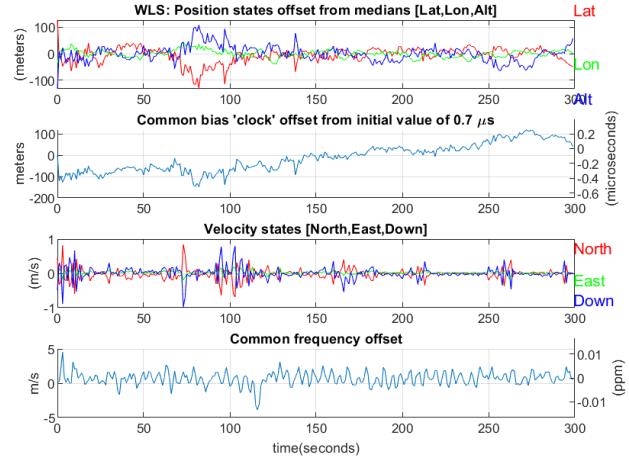


Figure 7. Optimal condition

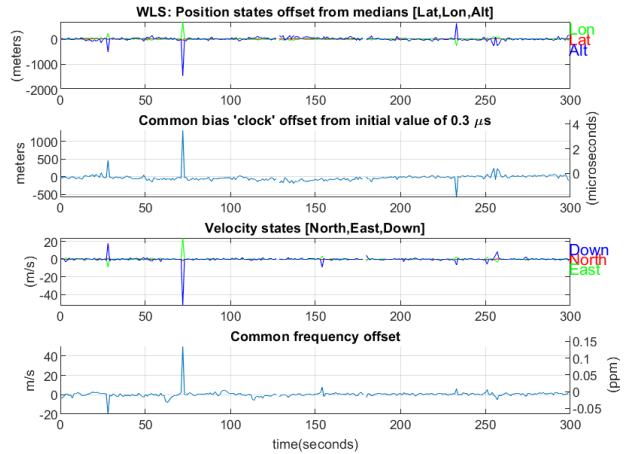


Figure 8. Battery save mode activated

3.3 Task 3: indoor.

An additional data collection attempt was carried out inside one of the classrooms at the Polytechnic in order to evaluate GNSS performance in indoor environments, where satellite signal reception is typically degraded. Despite conducting the measurement session for more than five minutes, the results were largely inconclusive. When processed and analyzed using MATLAB, the software was unable to generate any meaningful or continuous positional data from the session. Only two isolated position fixes were plotted, both of which were separated by an implausible distance of approximately 350 meters, as illustrated in Figure 9.

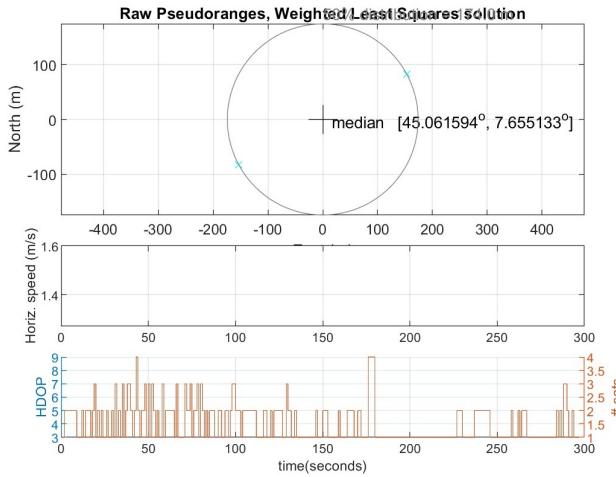


Figure 9.

This outcome highlights the severe limitations of GNSS signal acquisition indoors, where structural elements such as walls and ceilings significantly attenuate or block satellite signals. In such environments, the receiver may fail to maintain a stable lock on sufficient satellites, resulting in extremely sparse or erroneous data. The large spatial gap between the two recorded points likely reflects brief, unreliable signal acquisitions.

3.4 Task 5: spoofing positions.

This part of the study involved performing experiments under open-sky conditions, during which we simulated spoofing scenarios by deliberately altering specific signal parameters. Around the 15-second mark in the graph, there are noticeable sharp spikes in both positive and negative directions, as shown in Figure 10. These sudden fluctuations correspond to the initiation of the spoofing event, which causes the GNSS receiver to interpret the satellites as rapidly moving either toward or away from it. At that moment, the estimated satellite velocities shift from nearly 0 m/s up to approximately 2000 m/s, and then down to around -1500 m/s. This artificial variation is a direct result of the spoofing manipulation, leading the system to perceive an unrealistic change in satellite motion.

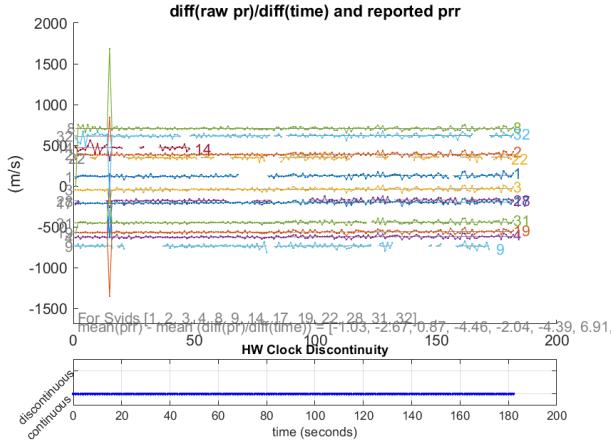


Figure 10.

The initial GNSS measurements were accurately recorded near the P lecture halls at the Polytechnic, reflecting the true starting location of the device. However, approximately 15 seconds into the data collection, a sudden and deliberate change in position occurs, shifting the estimated location to Piazza Adriano, as it can be seen from the Figure 11.



Figure 11.

Following this abrupt transition, all subsequent positional fixes consistently cluster around the spoofed location, demonstrating that the receiver was fully deceived by the introduced spoofing parameters. Notably, the data points after the spoofing onset also appear to be significantly more tightly grouped, indicating improved precision around the spoofed coordinates. This effect is clearly represented in Figure 12, where the spoofed location becomes the statistical median.

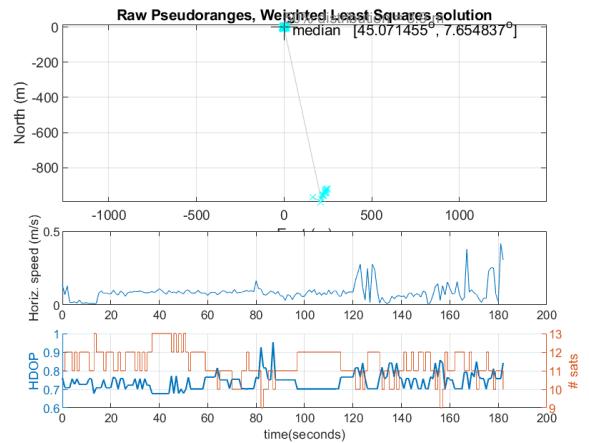


Figure 12.

3.5 Task 6: adding spoofing delay.

Using a spoofing delay, there are no differences in the final position. However, the behaviour of the Pseudorange vs Time plot, Figure 11, and the clock bias, Figure 12, change significantly. In the first it can be seen that the pseudoranges increase rapidly around 15s, which is the same aspect that happen in the common bias clock offset. After that, they remain constant without any fluctuations.

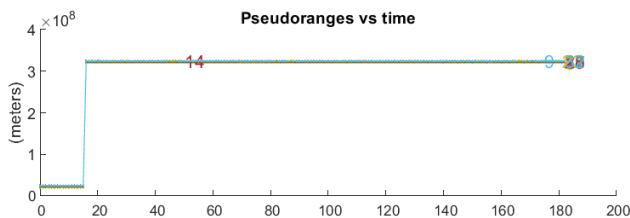


Figure 11.

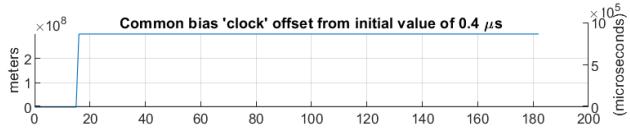


Figure 12.

This latter aspect is due to the fact that spoofing with delay manipulates not only the position but also the time of arrival, so the receiver will believe it is farther from all satellites. Comparing the two spoofing techniques, it can be stated that spoofing with delay is characterized by marked discontinuities in the data, whereas spoofing without delay is more subtle and continuous, making it more insidious but less detectable. Analyzing the graph of $\text{diff}(\text{raw pr})/\text{diff}(\text{time})$ it is observed that, in the case of spoofing with delay, Figure 13, an initial jump due to the delay is introduced, after which all the pseudorange evolve in a coherent way but with a fixed time offset, because all the satellites were "moved" simultaneously.

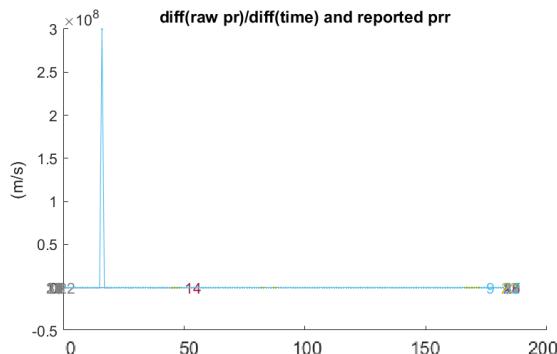


Figure 13.

On the other hand, in the spoofing position without delay, Figure 13, the pseudoranges appear modified in an uneven way: each satellite receives a different offset, making the data inconsistent with each other and making the satellites appear to be moving at relative physically incompatible speeds, resulting in severe mispositioning errors.

3.6 Task 7: adding interference source.

In this case, it was analyzed how a source of interference can modify the behaviour of GNSS measurement. In particular, in this case the device that is collecting data was called by another nearby smartphone, so in this scenario the GNSS receiver is affected by RF noise, which is typically generated during phone calls. During the call, the fact that there are shared hardware and the proximity of another device can, respectively, affects GNSS signal reception and introduce electromagnetic

interference. Then, the Figure 14, it's characterized by drops and oscillations due to the fact that a call introduces electromagnetic noise, so as a consequence the Carrier to noise ratio decreases.

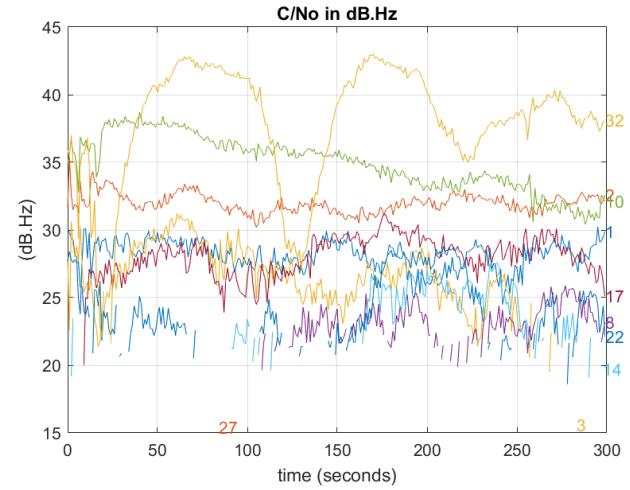


Figure 14.

Finally, in figure 15, which represent the horizontal speed, it is possible to observe fluctuations given by noise. This caused an instability in the Doppler measurement, which lowered the accuracy of the speed estimation.

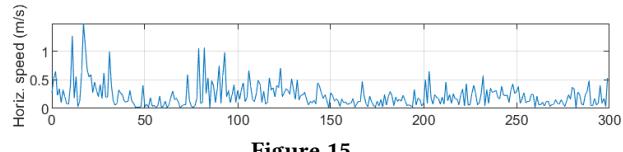


Figure 15.

4 CONCLUSION

In this report measurements were performed under different device states which leads to significant variations in the data obtained. Starting from optimal conditions, such as outdoor environments with clear satellite visibility, in which the data is accurate and reliable. Then, the same scenario was observed, but with battery saving mode, in which it was clear that, in order to save energy, the frequency of data update was lower. Moreover, the data obtained indoor led to the conclusion that there is the necessity to be on line of sight in order to get reasonable results. Furthermore, attacks such as spoofing and delayed spoofing were analyzed, first individually, and then by comparing them, underlining how they work and what their behaviors are. Finally, it was examined a case with a source of interference, which made evident that the noise can affect GNNS' performance .